FILED

SEP 9 2010

OFFICE OF THE CLERK

No. 10-352

# In The Supreme Court of the United States

THOMAS McCOY RICHARDSON,

*Petitioner,*

v.

UNITED STATES OF AMERICA,

*Respondent.*

On Petition for Writ of Certiorari to the
United States Court of Appeals
for the Fourth Circuit

## PETITION FOR WRIT OF CERTIORARI

Anthony G. Scheer
RAWLS, DICKINSON & SCHEER, P.A.
1011 East Morehead Street, Suite 300
Charlotte, North Carolina 28202
(704) 376-3200
tscheer@rdslaw.com

*Counsel of Record for Petitioner*

LANTAGNE LEGAL PRINTING
801 East Main Street Suite 100 Richmond, Virginia 23219 (800) 847-0477

## QUESTIONS PRESENTED

I. Were Richardson's Fourth Amendment rights violated when America Online, Inc. (AOL) searched his email account and reported to law enforcement that it found child pornography images, because AOL acted as an agent of law enforcement and no warrant authorized the unreasonable search?

II. Were Richardson's constitutional and statutory rights violated when the court granted America Online, Inc.'s motion to quash his subpoena duces tecum, foreclosing Richardson's ability to present facts relevant to his contention that AOL acted as an agent of law enforcement in searching his email?

## PARTIES TO THE PROCEEDING

1. Petitioner Thomas McCoy Richardson
2. Respondent United States of America.

## TABLE OF CONTENTS

Questions Presented ..... i

Parties to the Proceeding ..... i

Table of Contents ..... ii

Table of Authorities ..... iv

Opinions Below ..... 1

Jurisdiction ..... 1

Constitutional and Statutory Provisions ..... 2

Fourth Amendment to the United States Constitution ..... 2

14 U.S.C. § 13032 (amended and recodified in 18 U.S.C. § 2258A) ..... 2

Statement of the Case ..... 2

Factual Background ..... 2

Trial Court Proceedings ..... 5

Fourth Circuit Court of Appeals Proceedings ..... 8

Reasons for Granting the Petition ..... 8

This case presents an important federal question regarding the Fourth Amendment and privacy in the electronic age, and the Fourth Circuit's decision conflicts with relevant decisions of this Court ..... 8

The Motion to Quash ruling should be reviewed, because the Fourth Circuit decision sanctions a departure from the accepted and usual course of judicial proceedings and undermines the Fourth Amendment protections discussed above ..... 13

Conclusion ..... 17

Appendix:

Opinion of the United States Court of Appeals for the Fourth Circuit, decided June 11, 2010 ..... A1

Judgment of the United States District Court for the Western District of North Carolina, entered January 15, 2009 ..... A31

Order of the United States District Court for the Western District of North Carolina, entered January 16, 2008 ..... A46

Order of the United States District Court for the Western District of North Carolina, entered March 20, 2008 ..... A51

42 U.S.C.A. § 13032 ..... A58

## TABLE OF AUTHORITIES

### Cases

*Brady v. Maryland*, 373 U.S. 83 (1963) ..... 16

Skinner v. Railway Labor Executives, Ass'n, 489 U.S. 602 (1989) ..... 9

*United States v. Forrester*, 495 F.3d 1041 (9th Cir. 2007) ..... 8

*United States v. Nixon*, 418 U.S. 683 (1974) ..... 15

*United States v. Richardson*, 607 F.3d 357 (4th Cir. 2010) ..... 1

*Warshak v. United States*, 490 F.3d 455 (6th Cir. 2007), *vacated on other grounds*, 532 F.3d 521 (6th Cir. 2008) ..... 8

### Constitutional Provisions

U.S. Const. amend. IV ..... i, 2

### Statutes

14 U.S.C. § 13032 ..... 2, 3, 11

18 U.S.C. § 2252A(a)(5) ..... 6

18 U.S.C. § 2258A ..... 2, 3, 11

18 U.S.C. § 3231 ..... 6

28 U.S.C. § 1254 ..... 1

28 U.S.C. § 1291 ..... 8

**Rules**

F. R. Cr. P. 17 ..... 15

Fed. R. Ev. 803 ..... 15

Sup. Ct. R. 10 ..... 12, 16

Sup. Ct. R. 13 ..... 1

**Articles**

Schuyler B. Sorosky, Note, United States v. Forrester: *An Unwarranted Narrowing of the Fourth Amendment*, 41 Loy. L.A. L. Rev. 1121 (2008)..... 9

## OPINIONS BELOW

The Fourth Circuit Court of Appeals' opinion was filed on June 11, 2010 and is reported at *United States v. Richardson,* 607 F.3d 357 (4th Cir. 2010). The opinion is reprinted in the Appendix, p. A1.

The Western District of North Carolina's order granting AOL's motion to quash was filed on January 16, 2008 and was not reported. The order is reprinted in the Appendix, p. A46.

The Western District of North Carolina's order denying Petitioner's motion to suppress was filed on March 21, 2008 and was not reported. The order is reprinted in the Appendix, p. A51.

## JURISDICTION

Petitioner Richardson prays this Honorable Court review the Fourth Circuit Court of Appeals published opinion issued on June 11, 2010, affirming the trial court orders (1) denying his motion to suppress and (2) granting AOL's motion to quash his subpoena.

This Petition is filed within the time frame prescribed by Rule 13 of the Supreme Court Rules. This Court has jurisdiction pursuant to 28 U.S.C. § 1254.

## CONSTITUTIONAL AND STATUTORY PROVISIONS

### Fourth Amendment to the United States Constitution

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

### 14 U.S.C. § 13032 (amended and recodified in 18 U.S.C. § 2258A)

Pursuant to this Court's Rule 14.1(f), the text of 42 U.S.C. § 13032 is contained in the Appendix, p. A58.

## STATEMENT OF THE CASE

### Factual Background

America Online, Inc. (AOL) uses several methods to detect child pornography in subscriber emails and Internet browsing. When detected material appears to contain child pornography, AOL reports the find to the Cyber Tip Line at the National

Center for Missing and Exploited Children (NCMEC), as mandated by federal law. 14 U.S.C. § 13032 (amended and recodified in 18 U.S.C. § 2258A). One AOL detection method is an Image Detection and Filtering Program (IDFP) that recognizes and compares digital markings of files attached to a customer's email. Although the IDFP was discussed in the trial court and in the Fourth Circuit opinion, AOL did not claim IDFP was the detection method in this case.

AOL has publicly claimed to be in partnership with law enforcement. In 2006 written testimony before a House of Representatives Subcommittee, AOL Chief Counsel John Ryan spoke of AOL as "long partnered with law enforcement" and "work[ing] very closely with local, state, and federal law enforcement agencies to track down and prosecute child predators." (J.A. 157 and 167.) In this case, AOL filed a Motion to Quash Richardson's subpoena duces tecum. In the Motion, AOL stated that the company acted in "obedience to federal law" in its activities regarding the reporting of child pornography. (J.A. 61.) The record demonstrates that AOL was intertwined with law enforcement in the prosecution of child pornography laws. AOL worked directly with NCMEC (an arm of law enforcement) to create the reporting system that it and other ISP's used to discover and report illicit images. AOL managers sat on the board of directors of NCMEC, partnered with the federal Department of Justice's

Internet Crimes Against Children Task Force, and gave training and litigation support to various law enforcement agencies and their umbrella organizations. AOL even characterized its own in-house group working with law enforcement agencies as its "criminal investigations staff." (J.A. 29-32.)

Richardson was an AOL customer. He used the email addresses knifeisland@aol.com and tr1029@aol.com, and the screen name tr1029. On June 10, 2004, AOL detected the transmission of a child pornography image on the email address, knifeisland@aol.com. The company reported the detection to NCMEC, which passed the information to the North Carolina State Bureau of Investigation (SBI). As a result, the SBI issued an administrative subpoena for AOL to produce the relevant subscriber information. AOL provided Richardson's name and address. Several weeks later, SBI agents went to the address, but Richardson had moved.

Approximately a year later, AOL detected two emails on one day with child pornography on Richardson's other email account, tr1029@aol.com. AOL again reported its detection to NCMEC, which passed the information to the SBI. The SBI served another administrative subpoena. AOL responded that the email account was registered to Richardson at a Park Road, Charlotte, North Carolina address. The Park Road address, however, was a UPS store, not a residence. Through Richardson's driver's license, the SBI linked him to the UPS store and an

Andover Woods, Charlotte, North Carolina address. The SBI investigation also determined that Richardson had two 1996 South Carolina convictions and had previously been a registered sex offender.

On November 17, 2005, SBI Agent J.D. White applied for a search warrant for Richardson's Andover Woods home, primarily to search for evidence that he used his computer to view, store, and transmit images of child pornography. In support of the search warrant application, Agent White recounted AOL's detection and the related subscriber information that AOL provided in response to the administrative subpoena. No other information in the warrant application related specifically to Richardson, although Agent White recounted information about his training and experience of persons who view these images. The North Carolina magistrate issued the search warrant.

Law enforcement officers executed the search warrant on Richardson's Andover Woods home the same day. They recovered a computer. Richardson told officers he was the only person who used the computer and admitted that he sent and received child pornography by email. The computer contained 28 images and 21 video files of child pornography.

## Trial Court Proceedings

On April 26, 2006, Petitioner Richardson was charged with federal criminal offenses in a three-

count indictment returned by the Grand Jury in the Western District of North Carolina, Charlotte Division. A superseding indictment was returned on October 24, 2006. Richardson was charged with attempting to transport child pornography in interstate commerce, transporting child pornography in interstate commerce, and possessing child pornography that had been transported in interstate commerce, all by computer. The offenses violated 18 U.S.C. § 2252A(a)(5). The District Court exercised subject matter jurisdiction pursuant to 18 U.S.C. § 3231.

On July 4, 2007, Richardson moved to suppress all evidence gained as a result of AOL's searching his emails, including the emails and any evidence obtained in the search of his apartment, including his statements. Richardson argued that AOL engaged in an unconstitutional warrantless search of his private emails, in violation of his Fourth Amendment rights, because AOL conducted the search and reported the results as an agent of law enforcement. He also argued that the North Carolina magistrate lacked probable cause to issue the warrant, because the information about his alleged activities was stale and there was no probable cause to believe evidence of child pornography would be in his apartment when the warrant issued.

Through counsel, Richardson issued a subpoena duces tecum to AOL, seeking records regarding the detection and reporting of child pornography

in emails or Internet browsing. On January 4, 2008, one business day before the hearing, AOL moved to quash the subpoena on the grounds that it was overbroad and compliance would be unreasonable or oppressive.

On January 7, 2008, the Honorable Magistrate Judge David Keesler conducted a hearing on Richardson's motion to suppress and AOL's motion to quash. He concluded that Richardson did not carry his burden to establish that AOL acted as an agent or instrument of law enforcement, and noted that the discovery resulted from routine scanning. Judge Keesler granted the motion to quash. He concluded that the subpoena was unreasonably broad and that Richardson had not shown that the information sought was relevant, admissible, and specific. The district court adopted the rulings.

On April 3, 2008, Richardson entered a plea to two of the three counts before Magistrate Judge Keesler. The Plea Agreement provided that the Government would dismiss the third count. Further, Richardson preserved his right to appeal the trial court's rulings on the pretrial motions. On January 6, 2009, Presiding District Court Judge Martin Reidinger found that a factual basis existed for the plea, accepted the plea, and conducted a sentencing hearing. Judge Reidinger imposed 180-month concurrent sentences on the remaining two counts, with lifetime supervised release.

On January 14, 2009, Richardson filed written notice of appeal to the Fourth Circuit.

**Fourth Circuit Court of Appeals Proceedings**

Upon Richardson's timely appeal, the Fourth Circuit Court of Appeals reviewed the trial court decisions on the motions to suppress and to quash. On June 11, 2010, it affirmed the trial court rulings. The Court of Appeals exercised jurisdiction pursuant to 28 U.S.C. § 1291.

## REASONS FOR GRANTING THE PETITION

### This case presents an important federal question regarding the Fourth Amendment and privacy in the electronic age, and the Fourth Circuit's decision conflicts with relevant decisions of this Court.

Email has largely replaced physical mail as the primary written communication between citizens. Americans have a reasonable expectation of privacy in email communications that are not stored on a remote server. See, e.g., *Warshak v. United States,* 490 F.3d 455 (6th Cir. 2007), *vacated on other grounds,* 532 F.3d 521 (6th Cir. 2008). (Finding a reasonable expectation of privacy in email) and *United States v. Forrester,* 495 F.3d 1041 (9th Cir. 2007) (holding that IP addresses and email volume

are not protected by the Fourth Amendment.) Because Internet communications now penetrate the fabric of American life, citizens are justifiably concerned about email privacy, including privacy from governmental intrusion. See, e.g., Schuyler B. Sorosky, Note, United States v. Forrester: *An Unwarranted Narrowing of the Fourth Amendment*, 41 Loy. L.A. L. Rev. 1121 (2008). While the framers of the constitution could not have imagined modern communication, constitutional limits do not vanish in cyberspace.

In this case, AOL searched Richardson's correspondence in a way designed to reveal content of emails and their attachments. This intrusion constitutes a search of Richardson's email. Private party searches do not implicate the Fourth Amendment unless the private party acts as an instrument or agent of the Government. *Skinner v. Railway Labor Executives, Ass'n,* 489 U.S. 602 (1989). In searching subscriber's emails, Richardson's in particular, AOL sought to discover possible child pornography and report such finds to law enforcement. The question presented here is whether AOL's acted as an agent or instrument of the government so as to implicate the Fourth Amendment prohibitions against unreasonable, warrantless searches.

This Court found an agency relationship on analogous facts in *Skinner v. Railway Labor Executives, Ass'n,* 489 U.S. 602 (1989). *Skinner* involved two federal regulations regarding testing railway

employees for alcohol or controlled substances. Regulation Subpart C "Post-Accident Toxicological Testing," mandated breath and urine testing for railway employees involved in major train accidents and specified the manner of the testing. The search in Richardson's case was not mandated and is therefore distinguishable from the first regulation in *Skinner*, Subpart C. Like the statutes in this case, however, the second *Skinner* regulation was permissive not mandatory and was found to implicate Fourth Amendment protections. Regulation Subpart D, "Authorization to Test," authorized railway supervisors to compel breath and urine testing after a reportable accident or incident if a supervisor had a "reasonable suspicion" that the employee's conduct contributed or if the supervisor had a reasonable suspicion based on personal observations that the employee was impaired. *Id.* at 611. This Court held that both regulations implicated the Fourth Amendment, even Subpart D's non-mandatory testing. The Court said, "The fact that the Government has not compelled a private party to perform a search does not, by itself, establish that the search is a private one." *Id.* at 615. The Court found that the Government's conduct, as authorized by the regulations, was more than "a passive position toward the underlying private [search by railway companies]." The Fourth Amendment, said the Court, was implicated by the Government's "encouragement, endorsement, and participation." *Id.*

Current federal law does not mandate warrantless email searches. But like Subpart D in *Skinner*, federal law clears a path for Internet Service Providers ("ISP's") to search for child pornography by immunizing providers from any liability they might incur as a result of the searches, mandating that evidence gained during such searches be reported, and penalizing providers for failing to report child pornography on their networks. 14 U.S.C. § 13032 (amended and recodified in 18 U.S.C. § 2258A). This ISP reporting is the first step in investigating and prosecuting crimes, just as Subpart D in *Skinner* was the first step in criminal proceedings against railway employees. While the ISP reporting statute does not expressly create an agency relationship between ISPs and law enforcement, the facts of this case show that a specific, or *de jure,* agency relationship existed between AOL and law enforcement. AOL itself acknowledged that it acted "in obedience to federal law" in searching Richardson's emails. (J.A. 61.)

Although the Government did not compel or physically participate in AOL's search of Richardson's email, it encouraged and endorsed the search by using the fruits of that search to obtain administrative subpoenas that compelled AOL to produce subscriber identifying information. The Government encouraged the search as the first step in the criminal proceedings against Richardson. Like the regulation considered in *Skinner,* the reporting require-

ment here immunizes ISP's from liability for scanning Richardson's email and reporting the results to law enforcement. In addition, like the *Skinner* regulations, the federal reporting requirements preempt state law. In *Skinner,* these factors combined to implicate Fourth Amendment protections even for non-mandatory searches by the railway executives. Here, the totality of the statutes relating to ISP detection and reporting of child pornography predictably results in a governmental encouragement to search. The law imposes a burden to report, penalizes ISPs who fail to report, and eliminates any liability for these ISP searches.

In Richardson's appeal, the Fourth Circuit held that AOL acted as a private party. Considering the totality of the circumstances, however, the statute that allows AOL and other ISP's to engage in these searches, is analogous to the statute in *Skinner.* The Fourth Circuit's holding conflicts with this Court's holding in *Skinner* and this petition should therefore be granted. Sup. Ct. R. 10

Further, this Court has not, but should, settle the question of how the Fourth Amendment protections apply in email and other electronic communications. Therefore, this case presents an issue appropriate for review by writ of certiorari. *Id.*

**The Motion to Quash ruling should be reviewed, because the Fourth Circuit decision sanctions a departure from the accepted and usual course of judicial proceedings and undermines the Fourth Amendment protections discussed above.**

To support his motion to suppress, Richardson sought to present the trial court with AOL records that showed the link between AOL and law enforcement and established the agency relationship that implicated the Fourth Amendment. Richardson's subpoena duces tecum asked for AOL to bring:

> [A]ll records (including but not limited to emails, postal correspondence, minutes/notes of meetings, memoranda, and public relations material, and Congressional testimony) relating to AOL's coordination of efforts, training and/or strategic partnerships with all agencies of the [U.S.] Department of Justice, ... Postal Service, the Secret Service, the Internet Crimes Against Children Task Force ... and the [NCMEC], regarding the detection and reporting of child pornography content

> in emails and/or web browsing activity by AOL subscribers or on its network.

The record submitted in support of the Motion to suppress had established a close working relationship between AOL and federal law enforcement. Richardson had submitted evidence that, among other ties, AOL itself claimed that it had "long partnered with law enforcement," that it "work[ed] closely with local, state and federal law enforcement to track down and prosecute child predators," and that in searching customer emails for child pornography, it was "acting in obedience to federal law." (J.A. 61.) The subpoena sought the underlying facts to these relationships as claimed by AOL itself.

Richardson's attorney attempted to narrow the original subpoena before issuing it by contacting AOL to discuss the request. AOL's lawyers interposed the legal argument that because they were not a governmental agent, there was no information to subpoena. When the Magistrate Judge asked for a proposal to narrow the subpoena, Richardson's attorney asked that the court issue a subpoena to identify the individuals who managed these self-proclaimed partnerships with law enforcement, and for the records of those liaisons. The Magistrate, the District Court, and the Fourth Circuit all failed to address that narrowed subpoena.

In criminal proceedings, a subpoena duces tecum is intended not for pretrial discovery but to pro-

vide pretrial inspection in order to expedite the trial. *United States v. Nixon,* 418 U.S. 683, 689-699 (1974). Therefore, the subpoena must seek material that is (1) relevant, (2) admissible, and (3) specific. *Id.* at 700. Contrary to the Fourth Circuit's holding, Richardson's subpoena satisfies the three requirements.

First, the subpoena sought only material relevant to illuminate AOL's own claim to partnership with law enforcement. The material is relevant to the question of whether AOL was acting as a governmental agent. The subpoena specifically asked for material "relating to AOL's coordination of efforts, trainings[,] and/or strategic partnerships [with law enforcement], regarding the detection and reporting of child pornography . . . ." The request was based on AOL's public statements. Thus the first prong — relevance — is satisfied. The second prong — admissibility — is also satisfied on these facts, because the subpoena seeks AOL records, which are admissible as records kept in the ordinary course of business. Fed. R. Ev. 803(6). Finally, the subpoena (particularly the narrowed subpoena proposal by Richardson) satisfies the third prong — specificity— because the request is specific and includes a list of specifically named document types.

Rule 17 of the Federal Rules of Criminal Procedure allows a court to quash or modify a subpoena if compliance would be unduly burdensome. Richardson proposed in the alternative that AOL be

compelled to identify the managers who oversaw those partnerships with law enforcement. Modifying the subpoena this way would have created a narrower request that those few individuals produce the records supporting AOL's public statements. In failing to address the question of what burden Richardson's narrowed request placed on AOL, the courts below denied him access to relevant and admissible evidence without properly addressing the balancing test in *Nixon*.

Criminal defendants are generally entitled to discover exculpatory evidence. *Brady v. Maryland*, 373 U.S. 83 (1963). On these facts, the subpoena sought material that was tantamount to exculpatory evidence. The material was likely to defeat a part of the Government's case against Richardson — the fruits of AOL's search. AOL's court-sanctioned ability to conceal the information through quashing the subpoena deprived Richardson of his ability to fully present his agency claim on the motion to suppress. Even assuming the subpoena was burdensome, a lesser alternative was available through a narrowed subpoena. Neither the trial court nor the Fourth Circuit addressed the possibility of a narrowed subpoena that would protect Richardson's rights. The Fourth Circuit's ruling departs from the accepted and usual course of judicial proceedings and this case presents an issue appropriate for review by writ of certiorari. Sup. Ct. R. 10.

## CONCLUSION

The issue of ISP providers' searching subscriber's digital communications presents the question of how the Fourth Amendment applies in the electronic age. The relevant statutes and AOL's conduct in this case present the question of when an ISP provider acts as an agency of law enforcement in searching a subscriber's communications. These are important federal law questions and the Fourth Circuit's decision in this case conflicts with relevant decisions of this Court. Further, the Fourth Circuit's ruling on Richardson's motion to quash departs from usual and accepted judicial processes that permit an individual to review exculpatory material before trial. Therefore, this Court should grant this Petition.

Respectfully submitted, this 9th day of September 2010.

s/ Anthony G. Scheer
Anthony G. Scheer
Attorney for Petitioner
Rawls, Dickinson, &
Scheer, P.A.
1011 East Morehead
Street, Suite 300
Charlotte, NC 28204
704-376-3200
tscheer@rdslaw.com

No. _____

# In The Supreme Court of the United States

THOMAS McCOY RICHARDSON,

*Petitioner,*

v.

UNITED STATES OF AMERICA,

*Respondent.*

On Petition for Writ of Certiorari to the
United States Court of Appeals
for the Fourth Circuit

## APPENDIX

Anthony G. Scheer
RAWLS, DICKINSON & SCHEER, P.A.
1011 East Morehead Street, Suite 300
Charlotte, North Carolina 28202
(704) 376-3200
tscheer@rdslaw.com

*Counsel of Record for Petitioner*

LANTAGNE LEGAL PRINTING
801 East Main Street Suite 100 Richmond, Virginia 23219 (800) 847-0477

**PUBLISHED**
**UNITED STATES COURT OF APPEALS**
**FOR THE FOURTH CIRCUIT**

| | |
|---|---|
| UNITED STATES OF AMERICA,<br><br>*Plaintiff-Appellee,*<br><br>v.<br><br>THOMAS MCCOY RICHARDSON, JR.,<br><br>*Defendant-Appellant.* | No. 09-4072 |
| AOL LLC,<br>*Amicus Supporting Appellee.* | |

Appeal from the United States District Court for the Western District of North Carolina, at Charlotte.
Martin K. Reidinger, District Judge.
(3:06-cr-00085-MR-1)

Argued: March 24, 2010
Decided: June 11, 2010

Before TRAXLER, Chief Judge, and WILKINSON and DUNCAN, Circuit Judges.

---

Affirmed by published opinion. Chief Judge Traxler wrote the opinion, in which Judge Wilkinson and Judge Duncan joined.

---

## COUNSEL

**ARGUED**: Anthony Glen Scheer, RAWLS, DICKINSON & SCHEER, PA, Charlotte, North Carolina, for Appellant. Amy Elizabeth Ray, OFFICE OF THE UNITED STATES ATTORNEY, Asheville, North Carolina, for Appellee. **ON BRIEF**: Edward R. Ryan, United States Attorney, Charlotte, North Carolina, for Appellee. Christopher G. Bubb, Vice President, General Counsel, John R. LoGalbo, Assistant General Counsel, AOL LLC, Dulles, Virginia, for Amicus Supporting Appellee.

---

## OPINION

TRAXLER, Chief Judge:

Thomas McCoy Richardson, Jr., pled guilty to violating 18 U.S.C. § 2252A(a)(1) & (b)(1) by "knowingly transport[ing] and ship[ping] in interstate and foreign commerce, by means of a computer, child pornography," J.A. 16, and to violating 18 U.S.C. § 2252A(a)(5) by "knowingly possess[ing] ma-

terial that contained images of child pornography," J.A. 16. In doing so, Richardson preserved the right to appeal the district court's order denying his motion to suppress and quashing his subpoena duces tecum under Rule 17(c)(2) of the Federal Rules of Criminal Procedure.

On appeal, Richardson contends that AOL LLC ("AOL"), an internet service provider ("ISP") with whom he had an e-mail account, discovered the illegal images on which Richardson's child pornography charges were based by conducting an unconstitutional search on behalf of the Government. Richardson also contends that the search warrant subsequently executed at his Charlotte-area apartment was not supported by probable cause, rendering the evidence culled from his computer inadmissible. Finally, Richardson claims that the district court committed reversible error in granting AOL's motion to quash his subpoena seeking the production of documents that would establish an agency relationship between AOL and the Government with respect to the detection of AOL subscribers involved in child pornography. We conclude that the district court correctly rejected these arguments and affirm the district court.

I.

On June 10, 2004, AOL, pursuant to a mandatory reporting requirement set forth in 42 U.S.C. § 13032(b)(1),[1] reported to the Cyber Tip Line at the National Center for Missing and Exploited Children ("NCMEC") that AOL had detected the transmission of child pornography images by a subscriber using an e-mail address called knifeisland@aol.com. NCMEC, also as mandated by the same federal law, passed along this information to the North Carolina State Bureau of Investigation ("SBI"), which, in turn, served AOL with an administrative subpoena for subscriber information related to the "knifeisland@aol.com" address. AOL determined that the "knifeisland@aol.com" account was registered to Richardson at 2541 Pine View Lane, Apartment H, Gastonia, North Carolina. The screen name "tr2066" was also linked to this account. By August 2004, however, when SBI agents received and followed up on this information, Richardson no longer resided at the 2541 Pine View Lane address and no forwarding address was available.

The investigation of Richardson apparently stalled for about one year. Then, on September 2, 2005, AOL reported to NCMEC that it had detected the transmission of two e-mail messages con-

---

[1]This particular provision is no longer in effect. The reporting requirements were amended and are now codified in 18 U.S.C. § 2258A.

taining images depicting child pornography from an account named "tr1029@aol.com" by a person using the screen name "tr1029." NCSBI Agent J.D. White initiated an investigation following this second report. Pursuant to another administrative subpoena, AOL indicated that the "tr1029@aol.com" account was registered to Richardson at 8508 Park Road, Charlotte, North Carolina. The Park Road address, as it turned out, was the location of a UPS store. Further investigation by the NCSBI, however, revealed that Richardson was residing in Charlotte at 7805 Andover Woods Drive, Apartment 604, and linked Richardson through his driver's license to both the Park Road address of the UPS store (where Richardson had apparently received mail for a period of time) and the Pine View Lane address in Gastonia (where Richardson had established the knifeisland@aol.com account).

NCSBI agents researched Richardson's criminal history and discovered that Richardson was a registered sex offender in South Carolina as a result of two 1996 convictions. In the first instance, Richardson was arrested and charged with performing a lewd act upon a child under 14 years of age after he entered a Wal-Mart store in Florence, South Carolina, grabbed the buttocks of a minor girl, and uttered an obscene remark to her. He was ultimately convicted of assault and battery of a high and aggravated nature. In the second instance, Richardson was convicted for exposing himself as he walked through the same Wal-Mart.

On November 17, 2005, Agent White applied for a search warrant to search Richardson's Andover Woods Drive apartment in Charlotte primarily for evidence of Richardson's use of a computer to view, store, and transmit images of child pornography. In support of his probable cause showing, Agent White included the information disclosed by AOL pursuant to the administrative subpoenas and the details of the subsequent investigation conducted by NCSBI. Additionally, Agent White provided a summary of his background in criminal and computer investigation as well as his special training in the "investigation[ ] of child sexual exploitation and child pornography." J.A. 41. Based on his experience, Agent White indicated "[t]he use of computers to traffic in, trade, or collect child pornography has become one of the preferred methods of obtaining such materials . . . [because computers] provide[ ] a high degree of anonymity in obtaining child pornography . . . [and] a sense of privacy and secrecy not attainable by other media." J.A. 50. White further explained in his affi- davit that "[i]ndividuals involved in the possession and transportation of child pornography rarely, if ever, dispose of their sexually explicit materials," which "are extremely valuable to these individuals because of the difficulty, scarcity, expense, and danger involved in their collection." J.A. 50. Noting that even computer files that are deleted from the hard drive can be retrieved through a forensic examination of the computer, White asked the issuing judge to find "probable cause to believe that

Thomas Richardson's residence, 7805 Andover Woods Drive, Apartment 604, Charlotte, North Carolina, contains a computer or computers that have been used to communicate with individuals to acquire child pornography; store images of child pornography, and distribute images of child pornography." J.A. 51.

On November 17, 2005, law enforcement officers executed the search warrant for Richardson's Andover Woods apartment. The primary evidence recovered in the search was a computer. Richardson indicated that he was the sole user of the computer and admitted that he had sent and received child pornography by email. Richardson also told officers that he was "addicted to viewing [child pornography] over the Internet, but denied ever meeting or speaking by phone with anyone he met on the Internet under the age of 18." J.A. 211. A forensic examination of Richardson's computer revealed 28 images and 21 video files containing child pornography. Some of these images included depictions of adults engaged in illegal, obscene sexual acts with children between four and nine years of age.

Richardson moved to suppress both the evidence seized in the search of his home and his statements to law enforcement officers during the search. First, Richardson argued that in reporting the contents of his email, AOL was acting as an agent of the Government and had therefore conducted an unconstitutional warrantless search of his

private email communications. Second, Richardson argued that even if AOL had not acted as a law enforcement agent in reporting the emails, the issuing judge lacked probable cause to believe that evidence of a child pornography offense would be located at his apartment at the time of the search.

Subsequently, in hopes of obtaining documentary support for his argument that AOL was acting as an agent for the Government, Richardson served AOL with a subpoena duces tecum pursuant to Rule 17(c)(1) of the Federal Rules of Civil Procedure requesting that AOL produce

> all records (including but not limited to emails, postal correspondence, minutes/notes of meetings, memoranda, and public relations material, and Congressional testimony) relating to AOL's coordination of efforts, training and/or strategic partnerships with all agencies of the United States Department of Justice, the United States Postal Service, the Secret Service, the Internet Crimes Against Children Task Force with the Department of Justice, and the [NCMEC], regarding the detection and reporting of child pornography content in emails and/or web browsing activities by AOL subscribers or on its network.

J.A. 64.

In response to the subpoena, AOL filed a motion to quash on the grounds that the subpoena

was grossly overbroad in scope and that "compliance would be unreasonable or oppressive." Fed. R. Crim. P. 17(c)(2). AOL argued that Richardson's subpoena was essentially a fishing expedition "based on the unsupported legal theory that AOL is an *agent* of the United States," J.A. 58, and that compliance with the subpoena would require AOL "to carry out a search of its immense paper files and data bases seeking that which does not exist." J.A. 60.

In support of its motion to quash, AOL submitted a declaration from AOL Assistant General Counsel John R. LoGalbo primarily to show that there was no agency relationship between AOL and the Government. LoGalbo denied that law enforcement asked AOL to search Richardson's email or otherwise participate in the investigation of Richardson "except through the ordinary forms of compulsory legal process." J.A. 66. Instead, LoGalbo stated, AOL detected the illegal images attached to Richardson's email transmissions through AOL's Image Detection and Filtering Program ("IDFP"), one of several internally-developed scanning programs designed to keep AOL's systems secure. The IDFP, as summarized by the LoGalbo Declaration, recognizes and compares the digital "fingerprint" (known as a "hash value") of a given file attached to a subscriber's email with the digital "fingerprint" of a file that AOL previously identified as containing an image depicting child pornography. LoGalbo indicated that if the IDFP detected a match suggesting that an email transmission contained child pornog-

raphy images, then AOL notified the NCMEC as required by 42 U.S.C. § 13032. According to LoGalbo, "AOL developed and began using the IDFP in 2002 in order to protect its rights and property against lawbreakers, prevent the network from being used to carry or store contraband (i.e., illegal child pornography), and fulfill its legal obligation to report the transmission . . . of child pornography on its systems." J.A. 65.

The magistrate judge concluded that the subpoena was unreasonably broad and, therefore, that Richardson failed to show that all of the information sought by the subpoena was relevant, admissible, and specific. *See United States v. Nixon*, 418 U.S. 683, 698-700 (1974). The district court adopted the ruling of the magistrate judge.

The magistrate judge then recommended that Richardson's motion to suppress be denied. First, the magistrate judge concluded that the search warrant was supported by probable cause and rejected Richardson's argument that Agent White's affidavit failed to establish a sufficient nexus between evidence of the child pornography offense and the Andover Woods apartment where the warrant was executed. The magistrate judge found that, based both on the allegations specifically related to Richardson and the "general 'profile'" of child pornographers, J.A. 214, "there was a fair probability that the computer used by defendant for transmission of and storage of [child pornography] would be

found in his residence." J.A. 213. The district court adopted the recommendation of the magistrate judge.[2]

Second, the magistrate judge rejected Richardson's argument that AOL was acting as an agent for law enforcement and therefore conducted a warrantless search. In concluding that Richardson failed to carry his burden of establishing that AOL served as an agent or instrument of the government, the magistrate judge noted that AOL's "discovery of [child pornography] associated with [Richardson's] email account was the result of routine scanning the company conducts to recognize files that may be detrimental to AOL." J.A. 216. The district court adopted this recommendation as well.

Following the denial of his motion to suppress, Richardson pled guilty to transporting and shipping child pornography in violation of 18 U.S.C. §§ 2252A(a)(1) & (b)(1), and to possessing child pornography in violation of 18 U.S.C. § 2252A(a)(5). Under the terms of his plea agreement, Richardson preserved his right to appeal both the denial of his

---

[2] The magistrate judge also concluded that even if the warrant lacked probable cause, the good faith exception under *United States v. Leon*, 468 U.S. 897, 913 (1984), would apply. The district court, however, declined to reach the issue of whether the law enforcement officers acted in good faith.

motion to suppress and the granting of AOL's motion to quash.

II.

Richardson believes that AOL, functioning as a government agent, conducted a constitutionally impermissible search when it scanned his email communications for illicit images of child pornography without a search warrant. If AOL was a government agent, then probable cause and a warrant were required before any search was undertaken. If, however, AOL acted in a private capacity, then government activity is not implicated and the Fourth Amendment does not apply.

Assuming that AOL conducted a search within the meaning of the Fourth Amendment, we conclude that AOL's actions did not equate to governmental conduct triggering constitutional protection. The Fourth Amendment guarantees citizens the right to be free from "unreasonable searches and seizures." U.S. Const. amend. IV. But for a few exceptions, warrantless searches and seizures are "*per se* unreasonable." *Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973) (internal quotation marks omitted). The Fourth Amendment, however, does not protect against searches, no matter how unreasonable, conducted "by private individuals acting in a private capacity." *United States v. Jarrett*, 338 F.3d 339, 344 (4th Cir. 2003); *see United States v. Jacobsen*, 466 U.S. 109, 113 (1984). Rather, the Fourth Amend-

ment "proscrib[es] only governmental action," *Jacobsen*, 466 U.S. at 113, and thus "evidence secured by private searches, even if illegal, need not be excluded from a criminal trial," *United States v. Ellyson*, 326 F.3d 522, 527 (4th Cir. 2003) (internal quotation marks omitted).

However, when a private individual conducts a search "as an instrument or agent of the Government," *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 614 (1989), the limits imposed by the Fourth Amendment apply, *see Jarrett*, 338 F.3d at 344 ("The Fourth Amendment protects against unreasonable searches and seizures by Government officials and those private individuals acting as instruments or agents of the Government." (alterations and internal quotation marks omitted)). The defendant shoulders the burden of establishing the existence of an agency relationship—"a fact-intensive inquiry that is guided by common law agency principles." *Ellyson*, 326 F.3d at 527; *see Jarrett*, 338 F.3d at 344.

The question of whether a private entity such as AOL serves as a mere conduit for the Government in performing a search "necessarily turns on the degree of the Government's participation in the private party's activities." *Skinner*, 489 U.S. at 614. "[T]here must be some evidence of Government participation in or affirmative encouragement of the private search before a court will hold it unconstitutional. Passive acceptance by the Government is not

enough." *Jarrett*, 338 F.3d at 346. Additionally, we generally look for evidence bearing upon the question of "whether the private party's purpose for conducting the search was to assist law enforcement efforts or to further h[is] own ends." *Ellyson*, 326 F.3d at 527 (internal quotation marks omitted).

Thus, the key factors bearing upon the question of whether a search by a private person constitutes a Government search are: "(1) whether the Government knew of and acquiesced in the private search; and (2) whether the private individual intended to assist law enforcement or had some other independent motivation." *Jarrett*, 338 F.3d at 344. There is no question that law enforcement agents did not actually participate in the search at issue here. Richardson does not dispute LoGalbo's assertion that no law enforcement agency specifically asked AOL to search Richardson's email or provided information about Richardson to cause AOL to scan his emails. Neither did law enforcement officials request that AOL aid in the investigation of Richardson "except through the ordinary forms of compulsory legal process," *i.e.*, "two administrative subpoenas and a preservation request" served pursuant to the Stored Communications Act "for the purpose of identifying the name, address, and other subscriber identifying information for an AOL client." J.A. 66; *see* 18 U.S.C. § 2703. There is nothing in the record to suggest that, in fact, law enforcement agents were involved in the search or investigation of Richardson's email transmissions until af-

ter AOL reported its discoveries to NCMEC. Likewise, there is little evidence in this record to suggest that AOL intended to assist the Government in its case against Richardson. Without the unspecified discovery materials to which he believes he is entitled pursuant to the subpoena duces tecum quashed by the district court, Richardson is essentially forced to concede that there is little evidence in this record upon which to demonstrate the existence of a *de facto* agency relationship between AOL and the Government.

Instead, Richardson contends that by mandating AOL's compliance with the reporting scheme set forth in 42 U.S.C. § 13032, the Government actively encouraged the search of his email and transformed AOL into its agent. According to Richardson, the Government, by regulating ISP conduct, did not simply acquiesce to AOL's actions, but instead was actively involved in the search so as to "trigger[ ] Fourth Amendment protections, regardless of the private party's intentions." *Presley v. City of Charlottesville*, 464 F.3d 480, 488 n.7 (4th Cir. 2006).

Richardson draws an analogy to the Supreme Court's decision in *Skinner v. Railway Labor Executives' Association* for the basis of his argument. In *Skinner*, the Court considered whether the regulatory scheme imposed by the Federal Railroad Administration ("FRA") for mandatory and permissive drug testing by private railroads implicated the

Fourth Amendment. Subpart C of the regulations, entitled "Post-Accident Toxicological Testing," required railroads to gather blood and urine samples from employees involved in serious accidents resulting in fatalities, injuries or significant property damage. *See Skinner*, 489 U.S. at 609. Because the regulations in subpart C mandated the means, methods and procedures for testing, the Court concluded that "[a] railroad that complies with the provisions of Subpart C of the regulations does so by compulsion of sovereign authority, and the lawfulness of its acts is controlled by the Fourth Amendment." *Id.* at 614.

A more difficult question for the *Skinner* Court, however, was whether the Fourth Amendment was implicated when a private railroad tested its employees under certain non-mandatory regulations. Subpart D of the FRA's regulatory scheme, entitled "Authorization to Test for Cause," was permissive, authorizing breath or urine tests when a supervisor had a "'reasonable suspicion'" that a worker's actions "contributed to the occurrence or severity of [an] accident" or that an employee was "under the influence of alcohol." *Id.* at 611. Although permissive, Subpart D nevertheless dictated *how* the blood and urine tests were to be conducted: "As in the case of samples procured under Subpart C, the regulations set forth procedures for the collection of samples, and require[d] that samples be analyzed by a method that is reliable within known tolerances." *Id.* at 611-12 (internal quotation marks omitted). More-

over, the regulations "confer[red] upon the FRA the right to receive certain biological samples and test results procured by railroads pursuant to Subpart D." *Id.* at 615.[3]

The Court concluded that, despite the non-mandatory nature of Subpart D, a private railroad acts as a government agent when conducting breath or urine tests under that section:

> The fact that the Government has not compelled a private party to perform a search does not, by itself, establish that the search is a private one. Here, specific fea-

---

[3] Subpart D also prescribed formal procedures in the event samples procured under Subpart D were used for disciplinary purposes:

> Subpart D further provides that whenever the results of either breath or urine tests are intended for use in a disciplinary proceeding, the employee must be given the opportunity to provide a blood sample for analysis at an independent medical facility. § 219.303(c). If an employee declines to give a blood sample, the railroad may presume impairment, absent persuasive evidence to the contrary, from a positive showing of controlled substance residues in the urine. The railroad must, however, provide detailed notice of this presumption to its employees, and advise them of their right to provide a contemporaneous blood sample.

*Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 611 (1989).

> tures of the regulations combine to convince us that the Government did more than adopt a passive position toward the underlying private conduct.

*Id.* at 615. The Court explained that the Government's intent to actively participate and exert a measure of control over any search under Subpart D was apparent from the fact that the regulations preempted state law and "supersede[d] any provision of a collective bargaining agreement, or arbitration award construing such an agreement." *Id.* (internal quotation marks omitted). Additionally, the Court noted a private railroad was not permitted to "divest itself of, or otherwise compromise by contract, the authority conferred by Subpart D," and its employees were not "free to decline . . . to submit to breath or urine tests under the conditions set forth in Subpart D." *Id.*

Based on those provisions, the Court in *Skinner* concluded that any testing under Subpart D was not "primarily the result of private initiative" and thus triggered application of the Fourth Amendment. *Id.* The regulations in *Skinner* clearly demonstrated "the Government's encouragement, endorsement, and participation," *id.* at 615-16, by "remov[ing] all legal barriers" to such testing, by making clear the Government's "strong preference for testing" and "its desire to share the fruits of such intrusions," and by "mandat[ing] that the railroads not bargain away the authority to perform tests

granted by Subpart D." *Id.* at 615.

We reject Richardson's attempt to draw an analogy between the simple reporting requirement of § 13032 and the regulatory scheme at issue in *Skinner* authorizing a search. The version of § 13032 in effect when AOL reported Richardson required only that an ISP such as AOL report to the Cyber Tip Line at NCMEC in the event it "obtain[ed] knowledge of facts or circumstances from which a violation of section . . . 2252A . . . involving child pornography . . . [wa]s apparent." 42 U.S.C. § 13032(b)(1). Unlike the regulatory scheme at issue in *Skinner*, § 13032(b)(1) neither directed AOL to actively seek evidence of child pornography in certain circumstances nor prescribed the procedures for doing so in the event that AOL decided to ferret out subscribers using its system to transmit illegal digital images. In fact, Congress made abundantly clear that § 13032(b)(1) was not to be interpreted as requiring an ISP to monitor a subscriber's internet activity, explicitly stating that "[n]othing in this section may be construed to require a provider of electronic communication services or remote computing services to engage in the monitoring of any user, subscriber, or customer of that provider, or the content of any communication of any such person." 42 U.S.C. § 13032(e).

The extensive regulatory scheme at issue in *Skinner* suggested a "strong preference for testing," having eliminated "all legal barriers to the test-

ing." *Skinner*, 489 U.S. at 615. Indeed, the FRA's regulatory scheme forbade railroads from contracting away the authority to perform such tests via the collective bargaining process. By contrast, nothing in § 13032 precludes AOL or any other ISP from entering into subscriber agreements that actually preclude monitoring or the use of a scanning tool, nor does any portion of § 13032 remotely suggest a congressional preference for monitoring.

Moreover, the penalty provision for failure to report contained in § 13032 does not persuade us to the contrary. Richardson suggests that ISPs such as AOL would be compelled as a practical matter to monitor their subscribers in the face of substantial monetary fines imposed against "[a] provider . . . who knowingly and willfully fails to make a report" under § 13032(b)(1). 42 U.S.C. § 13032(b)(4).[4] As AOL points out, however, the converse is just as likely to be true, if not more so—if substantial fines are imposed for the failure to report known facts suggesting a violation of federal child pornography laws, ISPs and others subject to such penalties might just as well take steps to avoid discovering reportable information.

---

[4] An initial failure to report carried a fine of up to $50,000, while a subsequent failure carried a possible fine of $100,000. *See* 42 U.S.C. § 13032(b)(4).

Finally, we reject Richardson's argument that Congress' intent to deputize ISPs in the Government's effort to fight child pornography on the Internet is reflected by the immunity from civil liability afforded by § 13032(c). *See* 42 U.S.C. § 13032(c) ("No provider or user of an electronic communication service or a remote computing service to the public shall be held liable on account of any action taken in good faith to comply with or pursuant to this section."). Richardson believes this is especially true given the policy statements contained in the Communications Decency Act of a national policy "to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material" and "to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity . . . by means of computer." 47 U.S.C. §§ 230(b)(4) & (5).

The plain language of § 13032(c) clears the way for ISPs to *report* violations of the child pornography laws, not investigate them. The provision was clearly aimed at immunizing civil claims for mistaken and incorrect reports issued to the NCMEC and in no way encourages surreptitious searches. The Communications Decency Act is likewise of no assistance to Richardson, as it aims "to encourage service providers to self-regulate the dissemination of offensive material over their services" by protecting service providers from lawsuits casting them "in the role of a publisher." *Zeran v. America Online,*

*Inc.*, 129 F.3d 327, 331 (4th Cir. 1997).

We conclude that the statutory provision pursuant to which AOL reported Richardson's activities did not effectively convert AOL into an agent of the Government for Fourth Amendment purposes.

III.

We review the district court's order granting AOL's motion to quash under Rule 17(c) of the Federal Rules of Criminal Procedure for an abuse of discretion. *See United States v. Fowler*, 932 F.2d 306, 311 (4th Cir. 1991). In this context, an abuse of discretion occurs when the court uses an erroneous legal standard or bases its decision on clearly erroneous facts. *See United States v. Under Seal (In re Grand Jury)*, 478 F.3d 581, 584 (4th Cir. 2007).

The subpoena duces tecum issued by Richardson to AOL sought the production of essentially any document that would support his theory that AOL was in an agency relationship with the Government:

> YOU ARE . . . COMMANDED to bring with you the following document(s) or object(s): . . . [A]ll records (including but not limited to emails, postal correspondence, minutes/notes of meetings, memoranda, and public relations material, and Congressional testimony) relating to AOL's coordination of efforts,

> training and/or strategic partnerships with all agencies of the [U.S.] Department of Justice, . . . Postal Service, the Secret Service, the Internet Crimes Against Children Task Force . . . and the [NCMEC], regarding the detection and reporting of child pornography content in emails and/or web browsing activity by AOL subscribers or on its network.

J.A. 64.

Under Rule 17(c)(2), the court "may quash or modify" a subpoena duces tecum "if compliance would be unreasonable or oppressive." Fed. R. Civ. P. 17(c)(2). A subpoena is unreasonable or oppressive if it is "excessively broad" or "overly vague." *In re Grand Jury*, 478 F.3d at 584. In that vein, a fundamental concern is that the subpoena duces tecum is not intended to provide a means of pretrial discovery; rather, its primary purpose is simply "to expedite the trial by providing a time and place *before* trial for the inspection of subpoenaed materials." *Nixon*, 418 U.S. at 689-99; *see Fowler*, 932 F.2d at 311 (rejecting criminal defendant's application for a subpoena duces tecum in that it "was little more than a duplication of [his] discovery motion").

Richardson bears the burden under *Nixon* of showing that the material he has subpoenaed meets the requirements of "(1) relevancy; (2) admissibility; [and] (3) specificity." *Nixon*, 418 U.S. at 700. The subpoena duces tecum must be "made in good

faith and [must] not [be] intended as a general 'fishing expedition.'" *Id.*

Richardson contends that any information tending to show a partnership or agency relationship between AOL and the Government was highly relevant to his Fourth Amendment claim and that the district court's refusal to require compliance precluded him from developing this claim. While such information might indeed be relevant, Richardson fails to address the principal deficiency in his subpoena—the lack of specificity. Without it, Richardson is merely fishing for evidence that might support his theory, as if he were in the discovery phase of a civil action. Even on appeal, the phrasing of Richardson's argument—that "he should be allowed to discover the facts" supporting his theory that AOL and the Government were in a partnership—betrays his intention to misuse the subpoena *duces tecum* as a discovery mechanism to develop his agency claim. As we have explained consistently, "a Rule 17 subpoena *duces tecum* cannot substitute for the limited discovery otherwise permitted in criminal cases and the hope of obtaining favorable evidence does not justify the issuance of such a subpoena." *United States v. Caro*, 597 F.3d 608, 620 (4th Cir. 2010) (internal quotation marks omitted).

We conclude, therefore, that the district court did not abuse its discretion in granting AOL's motion to quash.

IV.

Finally, Richardson challenges the district court's conclusion that the search warrant was supported by probable cause. When considering a district court's denial of a suppression motion, we review factual findings for clear error and legal conclusions *de novo*. *See United States v. Blake*, 571 F.3d 331, 338 (4th Cir. 2009), *cert. denied*, 130 S. Ct. 1104 (2010). And, "[a]lthough we review de novo the denial of the motion to suppress by the district court, the determination of probable cause by the issuing magistrate is entitled to great deference from this court." *United States v. Hodge*, 354 F.3d 305, 309 (4th Cir. 2004). Our duty "'is simply to ensure that the magistrate had a substantial basis for concluding that probable cause existed.'" *Id.* (quoting *Illinois v. Gates*, 462 U.S. 213, 238-39 (1983)).

Although the concept of probable cause defies a precise definition, it "exist[s] where the known facts and circumstances are sufficient to warrant a man of reasonable prudence in the belief that contraband or evidence of a crime will be found" in the place to be searched. *Ornelas v. United States*, 517 U.S. 690, 696 (1996). A probable cause assessment requires the issuing judge to decide whether, given the totality of the circumstances, there is a "fair probability that contraband or evidence of a crime will be found in a particular place." *Gates*, 462 U.S. at 238.

Richardson contends that there was no probable cause because the information supporting the issuance of the search warrant was stale. *See United States v. McCall*, 740 F.2d 1331, 1335-36 (4th Cir. 1984) ("A valid search warrant may issue only upon allegations of facts so closely related to the time of the issue of the warrant as to justify a finding of probable cause at that time." (internal quotation marks omitted)); *id.* at 1336 ("[E]vidence seized pursuant to a warrant supported by 'stale' probable cause is not admissible in a criminal trial to establish the defendant's guilt."). In this regard, Richardson claims that the fatal flaw in Agent White's affidavit is that it failed to specify the date on which he possessed or emailed the illegal images; at most, Richardson contends, the supporting affidavit established probable cause that he possessed and distributed child pornography at some unspecified time in the past. Furthermore, Richardson suggests that the only information offered to the issuing judge to "freshen" the probable cause was boilerplate "profile" information about the general tendencies of child pornography collectors, *e.g.*, that "[i]ndividuals involved in the possession and transportation of child pornography rarely, if ever, dispose of their sexually explicit materials" and tend to store their collected materials in their "residence or other secure location to ensure convenient and ready access." J.A. 50. If Agent White's affidavit establishes probable cause, Richardson concludes, then the residence of anyone who has ever possessed or distributed any such materials at some point in the past will be subject to a

search so long as the supporting affidavit includes similar boilerplate language. *See United States v. Prideaux-Wentz*, 543 F.3d 954, 957, 958-59 (7th Cir. 2008) (concluding affidavit contained stale information despite description of "'child pornography collector characteristics'" where the government did not identify dates on which illegal images were uploaded and record indicated that images could have been obtained as much as four years prior to the warrant). We cannot agree.

Although "there is no question that time is a crucial element of probable cause," *McCall*, 740 F.2d at 1335, the existence of probable cause cannot be determined "by simply counting the number of days between the occurrence of the facts supplied and the issuance of the affidavit," *id.* at 1336 (internal quotation marks omitted). Instead, we "look to all the facts and circumstances of the case, including the nature of the unlawful activity alleged, the length of the activity, and the nature of the property to be seized." *Id.* In the context of child pornography cases, courts have largely concluded that a delay—even a substantial delay—between distribution and the issuance of a search warrant does not render the underlying information stale. This consensus rests on the widespread view among the courts—in accord with Agent White's affidavit—that "collectors and distributors of child pornography value their sexually explicit materials highly, 'rarely if ever' dispose of such material, and store it 'for long periods' in a secure place, typically in their homes." *United States*

*v. Lacy*, 119 F.3d 742, 746 (9th Cir. 1997); *see United States v. Watzman*, 486 F.3d 1004, 1008 (7th Cir. 2007) (rejecting challenge to probable cause where three months elapsed between the crime and issuance of the warrant where agent testified child pornographers retain their collected materials for long periods of time); *United States v. Gourde*, 440 F.3d 1065, 1072 (9th Cir. 2006) (en banc) (concluding that "[t]he details provided on the use of computers by child pornographers and the collector profile" provided support for a finding of probable cause); *United States v. Riccardi*, 405 F.3d 852, 861 (10th Cir. 2005) (finding probable cause based, in part, on "the observation that possessors often keep electronic copies of child pornography"); *United States v. Lemon*, 590 F.3d 612, 615 (8th Cir. 2010) ("Many courts, including our own, have given substantial weight to testimony from qualified law enforcement agents about the extent to which pedophiles retain child pornography."), *cert. denied*, No. 90-10170, 2010 WL 1531424 (May 17, 2010); *United States v. Morales-Aldahondo*, 524 F.3d 115, 119 (1st Cir. 2008) (holding that three-year delay between acquisition of child pornography and application for warrant did not render supporting information stale since "customers of child pornography sites do not quickly dispose of their cache"), *cert. denied*, 129 S. Ct. 512 (2008).

Here, the information provided by Agent White established that no more than four months had passed from the time that Richardson emailed

an image depicting child pornography using his "tr1029@aol.com" account until the warrant was issued on November 17, 2005. Although Agent White did not supply the precise date of the email transmission, he indicated that the "tr1029@aol.com" account was established by Richardson on July 22, 2005, and the offending email could thus not have been sent before that time. We conclude that a delay of four months does not preclude a finding of probable cause based on staleness in light of the other information supplied by Agent White, including the previous instance in which Richardson used an AOL account to send such images and Agent White's sworn statement that child pornographers "rarely, if ever, dispose of their sexually explicit materials," and that "even if a computer file is deleted from a hard drive or other computer media, a computer expert is still likely to retrieve . . . such files through scientific examination of the computer." J.A. 50.

Richardson raises one other challenge to the search warrant that is closely related to the idea of staleness. He contends that the affidavit failed to include any specific facts suggesting that evidence of these offenses would be found in the Andover Woods apartment. That is, Richardson argues the affidavit failed to establish a nexus with the place to be searched. According to Richardson, the only basis in the supporting affidavit for finding the required nexus to Richardson's Andover Woods apartment was the generic, boilerplate "child pornographer profile." Richardson believes that there must be some

"specific" allegation that he was keeping evidence of these crimes at the Andover Woods apartment—for example, that he was using the same computer at the new residence. We disagree.

Richardson's argument ignores the reasonable, commonsense inferences that an issuing magistrate is permitted to draw from the totality of the circumstances in assessing probable cause. As we have observed before, "the nexus between the place to be searched and the items to be seized may be established by the nature of the item and the normal inferences of where one would likely keep such evidence." *United States v. Anderson*, 851 F.2d 727, 729 (4th Cir. 1988). Agent White's affidavit linked Richardson's email accounts, which he used to distribute child pornography, to his previous and current (at the time of the warrant) addresses. The totality of the evidence, including this information, provided the issuing magistrate with a substantial basis for concluding that there was a fair probability that the computer Richardson used to engage in these unlawful activities was kept in his current residence.

V.

For the foregoing reasons, we affirm the order of the district court denying Richardson's motion to suppress and granting AOL's motion to quash the subpoena duces tecum.

*AFFIRMED*

**UNITED STATES DISTRICT COURT**
**FOR THE WESTERN DISTRICT OF**
**NORTH CAROLINA**

**UNITED STATES OF AMERICA**

**v.** **Case Number:**
**DNCW306CR000085-001**

**THOMAS McCOY RICHARDSON**

**JUDGMENT IN A CRIMINAL CASE**

The defendant, THOMAS McCOY RICHARDSON, was represented by Anthony G. Scheer.

The defendant pled guilty to count(s) 2 and 3. Accordingly, the court has adjudicated that the defendant is guilty of the following offense(s):

| Title and Section | Nature of Offense |
|---|---|
| 18: U.S.C. 2252(a)(1) and (b)A(1) and 2256(8)(A) | Transport and Ship Interstate and Foreign Commerce, by Means of a Computer, Child Pornography |

Date Offense Concluded: 9/1/05

Counts: 3

| Title and Section | Nature of Offense |
|---|---|
| 18: U.S.C. 2252A(a)(5) | Possession of Child Pornography Stored on a Computer Hard Drive that had been Transported by Computer over the Internet |

Date Offense Concluded: 11/17/05

Counts: 3

On motion of the United States, the court has dismissed cout(s) 1.

IT IS ORDERED that the defendant shall notify the United States Attorney for this district within 30 days of any change of name, residence, or mailing address until all fines, restitution, costs, and special assessments imposed by this judgment are fully paid. If ordered to pay monetary penalties, the defendant shall notify the court and United States attorney of any material change in the defendant's economic circumstances.

/s/ Martin Reidinger
Martin Reidinger
United States District Judge
Date: January 15, 2009

**IMPRISONMENT**

The defendant is hereby committed to the custody of the United States Bureau of Prisons to be

imprisoned for a term of ONE HUNDRED EIGHTY (180) MONTHS on each of counts 2 and 3, to served concurrently.

The court makes the following recommendations to the Bureau of Prisons:

The Defendant shall be allowed to participate in any available substance abuse treatment programs while incarcerated and if eligible receive benefit of 18: U.S.C. 3621(e)(2).

The Defendant shall participate in a sex offender treatment program while incarcerated, if eligible.

The Defendant shall be designated at Butner, NC. If not Practical, then as close to Columbia, SC as possible, and to a facility that is consistent with his security classification.

The Defendant shall participate in the Federal Bureau of Prison's Inmate Financial Responsibility Program.

The Defendant shall support all dependants from prison earnings while incarcerated.

The Defendant shall be given credit for time-served.

The defendant is remanded to the custody

of the United States Marshal.

**RETURN**

I have executed this Judgment as follows:

_____

_____

_____

_____

Defendant delivered on _____
To_____ At _____, with a certified copy of this Judgment.

United States Marshal

By

Deputy Marshal

**SUPERVISED RELEASE**

Upon release from imprisonment, the defendant shall be on supervised release for a term of LIFE on each of counts 2 and 3, to run concurrently.

- The Condition for mandatory drug testing is suspended based on the court's determination that the defendant poses a low risk of future substance abuse.

**STANDARD CONDITIONS OF SUPERVISION**

The defendant shall comply with the standard conditions that have been adopted by this court and any additional conditions ordered.

1. The defendant shall not commit another federal, state, or local crime.
2. The defendant shall refrain from possessing a firearm, destructive device, or other dangerous weapon.
3. The defendant shall pay any financial obligation imposed by this judgment remaining unpaid as of the commencement of the sentence of probation or the term of supervised release on a schedule to be established by the court.
4. The defendant shall provide access to any personal or business financial information as requested by the probation officer.
5. The defendant shall not acquire any new lines of credit unless authorized to do so in advance by the probation officer.
6. The defendant shall not leave the Western District of North Carolina without the permission of the Court or probation officer.
7. The defendant shall report in person to the probation officer as directed by the Court or probation officer and shall submit a truthful and complete written report within the first five days of each month.
8. A defendant on supervised release shall report

in person to the probation officer in the district to which he or she is released within 72 hours of release from custody of the Bureau of Prisons.

9. The defendant shall answer truthfully all inquiries by the probation officer and follow the instructions of the probation officer.
10. The defendant shall support his or her dependents and meet other family responsibilities.
11. The defendant shall work regularly at a lawful occupation unless excused by the probation officer for schooling, training, or other activities authorized by the probation officer.
12. The defendant shall notify the probation officer within 72 hours of any change in residence or employment.
13. The defendant shall refrain from excessive use of alcohol and shall not unlawfully purchase, possess, use, distribute or administer any narcotic or other controlled substance, or any paraphernalia related to such substances, except as duly prescribed by a licensed physician.
14. The defendant shall participate in a program of testing and treatment or both for substance abuse if directed to do so by the probation officer, until such time as the defendant is released from the program by the probation officer; provided, however, that defendant shall submit to a drug test within 15 days of release on probation or supervised release and at least two peri-

odic drug tests thereafter for use of any controlled substance, subject to the provisions of 18:3563(a)(5) or 18:3583(d), respectively.

15. The defendant shall not frequent places where controlled substances are illegally sold, used, distributed, or administered.
16. The defendant shall not associate with any persons engaged in criminal activity, and shall not associate with any person convicted of a felony unless granted permission to do so by the probation officer.
17. The defendant shall submit his person, residence, office or vehicle to a search, from time to time, conducted by any U.S. Probation Officer and such other law enforcement personnel as the probation officer may deem advisable, without a warrant; and failure to submit to such a search may be grounds for revocation of probation or supervised release. The defendant shall warn other residents or occupants that such premises or vehicle may be subject to searches pursuant to this condition.
18. The defendant shall permit a probation officer to visit him or her at any time at home or elsewhere and shall permit confiscation of any contraband observed by the probation officer.
19. The defendant shall notify the probation officer within 72 hours of defendant's being arrested or questioned by a law enforcement officer.
20. The defendant shall not enter into any agree-

ment to act as an informer or a special agent of a law enforcement agency without the permission of the Court.

21. As directed by the probation officer, the defendant shall notify third parties of risks that may be occasioned by the defendant's criminal record or personal history or characteristics, and shall permit the probation officer to make such notifications and to confirm the defendant's compliance with such notification requirement.
22. If the instant offense was committed on or after 4/24/96, the defendant shall notify the probation officer of any material changes in defendant's economic circumstances which may affect the defendant's ability to pay any monetary penalty.
23. If home confinement (home detention, home incarceration or curfew) is included you may be required to pay all or part of the cost of the electronic monitoring or other location verification system program based upon your ability to pay as determined by the probation officer.
24. The defendant shall cooperate in the collection of DNA as directed by the probation officer.

ADDITIONAL CONDITIONS:

25. The defendant shall have no direct or indirect contact, at any time, for any reason with the victim(s), the victim's family, or affected parties

in this matter unless provided with specific written authorization to do so in advance by the U.S. Probation Officer.

26. The defendant shall submit to a psycho-sexual evaluation by a qualified mental health professional experienced in evaluating and managing sexual offenders as approved by the U.S. Probation Officer. The defendant shall complete the treatment recommendations and abide by all of the rules, requirements, and conditions of the program until discharged. He shall take all medications as prescribed.
27. The defendant shall submit to risk assessments, psychological and physiological testing, which may include, but is not limited to a polygraph examination and/or Computer Voice Stress Analyzer (CVSA), or other specific tests to monitor his/her compliance with probation or supervised release and treatment conditions, at the direction of the U.S. Probation Officer.
28. The defendant's residence and employment shall be approved by the U.S. Probation Officer. Any proposed change in residence or employment must be provided to the U.S. Probation Officer at least 10 days prior to the change and pre-approved before the change may take place.
29. The defendant shall not possess any materials depicting and/or describing "child pornography" and/or "simulated child pornography" as defined in 18 U.S.C. § 2256, nor shall he/she enter

any location where such materials can be accessed, obtained or viewed, including pictures, photographs, books, writings, drawings, videos, or video games.

30. The defendant shall register and keep the registration current, in each jurisdiction where the offender resides, where the offender is an employee, and where the offender is a student. For initial registration purposes only, a sex offender shall also register in the jurisdiction in which convicted if such jurisdiction is different from the jurisdiction of residence.
31. The defendant shall not purchase, possess or control cameras, camcorders, or movie cameras without prior approval of the U.S. Probation Office.
32. The defendant shall not use, purchase, possess, procure, or otherwise obtain any computer or electronic device that can be linked to any computer networks, bulletin boards, internet, internet service providers, or exchange formats involving computers unless approved by the U.S. Probation Officer. Such computers, computer hardware or software is subject to warrantless searches and/or seizures by the U.S. Probation Office.
33. The defendant shall allow the U. S. Probation Officer, or other designee, to install software designed to monitor computer activities on any computer the defendant is authorized to use.

This may include, but is not limited to, software that may record any and all activity on computers the defendant may use, including the capture of keystrokes, application information, internet use history, email correspondence, and chat conversations. The defendant shall pay any costs related to the monitoring of his computer usage.

34. The defendant shall not use, possess, or control any bootable linux or counter forensic tools.
35. The defendant shall not have any social networking accounts without the approval of the U. S. Probation Officer.
36. During the period of probation or supervised release, the defendant shall notify his employers, family, friends, and others with whom he has regular contact of his conviction and/or history as a sex offender and that he/she is being supervised by a U.S. Probation Officer.
37. The defendant shall not engage in any forms of exhibitionism, voyeurism, obscene phone calls, or other lewd or lascivious behavior, nor shall he/she engage in any form of "grooming" behavior that is meant to attract, seduce, or reduce resistance or inhibitions of a potential victim.
38. The defendant shall not own, use or have access to the services of any commercial mail receiving agency or storage unit nor shall he/she open or maintain a post office box or storage unit without the prior approval of the U.S. Probation Of-

ficer. The defendant shall provide the U.S. Probation Office with a list of all P.O. Boxes and/or storage units to which he may have access.

39. The defendant shall not possess sado masochistic/MASO bindings, restraints, handcuffs, etc.
40. The defendant shall not possess children's clothing, toys, games, etc. without permission of the U.S. Probation Office.
41. The defendant shall not be employed in any position or participate as a volunteer in any activity that involves direct or indirect contact with children under the age of eighteen (18), without written permission from the U.S. Probation Officer. Under no circumstances may the defendant be engaged in a position that involves being in a position of trust or authority over any person under the age of eighteen (18).
42. The defendant shall not possess any legal or illegal pornographic material, nor shall he/she enter any location where such materials can be accessed, obtained, or viewed, including pictures, photographs, books, writings, drawings, videos, or video games.
43. The defendant shall maintain a telephone at the place of residence without any "call forwarding", "caller ID", "call waiting", modems, answering machines, cordless telephones or other special services for the above period. The defendant may be required to wear an electronic device or submit to another location veri-

fication system and shall observe the rules specified by the Probation Officer.

44. Throughout the period of supervision the probation officer shall consider the defendant's economic circumstance as it pertains to the defendant's ability to pay any monetary penalty ordered, and shall notify the Court of any changes, with modifications recommended, as appropriate.

## CRIMINAL MONETARY PENALTIES

The defendant shall pay the following total criminal monetary penalties in accordance with the Schedule of Payments.

| Assessment | Fine | Restitution |
|---|---|---|
| $200.00 | $0.00 | $0.00 |

## FINE

The defendant shall pay interest on any fine or restitution of more than $2,500.00, unless the fine or restitution is paid in full before the fifteenth day after the date of judgment, pursuant to 18 U.S.C. § 3612(g).

The court has determined that the defendant does not have the ability to pay interest and it

is ordered that the interest requirement is waived.

## COURT APPOINTED COUSEL FEES

No fees have been imposed in this case.

## SCHEDULE OF PAYMENTS

Having assessed the defendant's ability to pay, payment of the total criminal monetary penalties shall be due as follows:

B *X* Payment to begin immediately (may be combined with (D) below); or

D *X* Payment in equal Monthly (E.g. weekly, monthly, quarterly) installments of $ $50.00 To commence 60 (E.g. 30 or 60 days) after release from imprisonment to a term of supervision. In the event the entire amount of criminal monetary penalties imposed is not paid prior to the commencement of supervision, the U.S. Probation Officer shall pursue collection of the amount due, and may request the court to establish or modify a payment schedule if appropriate 18 U.S.C. § 3572.

No special instructions were given regard-

ing the payment of criminal monetary penalties.

Payments shall be applied in the following order: (1) assessment, (2) restitution principal, (3) restitution interest, (4) fine principal, (5) community restitution, (6) fine interest, (7) penalties, and (8) costs, including cost of prosecution and court costs.

**IN THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF NORTH CAROLINA**
**CHARLOTTE DIVISION**
**DOCKET NO. 3:06-CR-85-MR-DCK-1**

| | | |
|---|---|---|
| **UNITED STATES OF AMERICA,** | ) | |
| | ) | |
| **Plaintiff,** | ) | |
| | ) | |
| **v.** | ) | **ORDER** |
| | ) | |
| **THOMAS MCKOY RICHARDSON,** | ) | |
| | ) | |
| **Defendant.** | ) | |
| | ) | |

**THIS MATTER IS BEFORE THE COURT** on the "Motion By AOL LLC To Quash Subpoena (Rule 17)" (Document No. 31), filed January 4, 2008. This matter has been referred to the undersigned Magistrate Judge pursuant to 28 U.S.C. §636(b), and is now ripe for disposition. Having carefully considered the motion, the record, the applicable authority, and the arguments of the parties at a hearing on January 7, 2008, the undersigned will respectfully grant the motion to quash.

## I. BACKGROUND

In an effort to support his motion to sup-

press in this matter, Defendant issued a subpoena to "Ms. Abigail Abraham or Custodian of Records" at AOL, LLC on December 10, 2007. (Document No. 31-2). This subpoena was marked as received by the AOL legal department on December 12, 2007. The subpoena specifically commanded AOL to

> Appear and produce all records . . . relating to AOL's coordination of efforts[,] training and/or strategic partnerships with all agencies of the United States Department of Justice, the United States Postal Service, the Secret Service, the Internet Crimes Against Children Task Force within the Department of Justice, and the National Center for Missing and Exploited Children, regarding the detection and reporting of child pornography content in emails and/or web browsing activit[y] by AOL subscribers or on its network.
> . . .

AOL LLC ("AOL") filed its motion to quash the subpoena (Document No. 31) on January 4, 2008. The undersigned heard arguments on the motion on January 7, 2008 – the date previously set by the Court for argument on the Defendant's motion to suppress.

## II. DISCUSSION

Subpoenas in criminal cases are addressed in Rule 17 of the Federal Rules of Criminal Procedure. With regard to motions to quash, Rule 17(c)(2)

provides that "[o]n motion made promptly, the court may quash or modify the subpoena if compliance would be unreasonable or oppressive."

As an initial matter, the timing of the filing of this motion to quash does raise concerns as to whether the motion was "made promptly." At first blush, certainly the filing of the motion to quash on the afternoon of the last business day prior to the date the subpoenaed materials are to be produced for the Defendant's use in a hearing on his motion to suppress does stretch the boundaries of promptness. However, upon consideration of the arguments from the parties on this issue at the January 7, 2008 hearing, the undersigned is satisfied that the motion should not be denied on the basis of a lack of promptness.

Among other things, there appears to be no dispute that the parties had engaged in at least two lengthy conversations in the months prior to the motion's filing attempting to resolve the matter. Although a more timely filing of the motion would have been preferable, it is clear to the undersigned that Defendant fully anticipated the motion to quash and that Defendant therefore was not unreasonably disadvantaged by its filing. Furthermore, in an effort to be as fair as possible, the undersigned at the January 7, 2008 hearing offered the Defendant the opportunity to file a written response to the motion to quash, and the Defendant declined.

We thus turn to the merits of the motion. AOL's motion to quash includes an affidavit from its Assistant General Counsel, John R. LoGalbo. (Document No. 31-3). Mr. LoGalbo's affidavit essentially describes tools AOL uses to protect its network and customers from detrimental files. The affidavit describes the scanning tools and hash values that AOL developed to proactively detect child pornography. The affidavit explains that if AOL identifies files with child pornography through the use of its scanning tools, it is required by 42 U.S.C. 13032 to notify the National Center for Missing and Exploited Children ("NCMEC"). Mr. LoGalbo seems to deny any coordination between AOL and any law enforcement agency in detecting child pornography. AOL takes the position that the documents the Defendant seeks do not exist – and that conducting the search to confirm that fact will be unreasonable and oppressive.

Defendant contends that the subpoena served on AOL should be enforced. The Defendant wants these documents because he believes they might support one of the alternative theories in his motion to suppress – that AOL acted as an agent of federal law enforcement, and in that agency capacity, conducted an unconstitutional search by using the scanning tools. The Defendant argues that AOL should not be allowed to quash the subpoena simply because its attorneys contend the requested materials do not exist. The Defendant makes an articulate and creative argument in support of his theory; nev-

ertheless, in the end, the undersigned finds that the subpoena is overly broad and should be quashed.

Rule 17(c)(2) allows a subpoena to be quashed or modified if "compliance would be unreasonable or oppressive." In United States v. Nixon, 418 U.S. 683 (1974), the Supreme Court observed that Rule 17(c) "was not intended to provide a means of discovery for criminal cases" and that the issuer of a subpoena has the burden to demonstrate that the information sought is relevant, admissible, and specific. Nixon, 418 U.S. at 698-700; see also United States v.Hang, 75 F.3d 1275, 1283 (8th Cir. 1996). The undersigned has considered, and at the hearing explicitly opened the door for Defendant to suggest, a modification of the subpoena, but Defendant failed to suggest a satisfactory alternative to the subpoena as originally drafted. In the view of the undersigned, under prevailing law, the subpoena is unacceptably broad, thus making compliance "unreasonable or oppressive." It must be quashed.

## III. CONCLUSION

**IT IS THEREFORE ORDERED** that the "Motion By AOL LLC To Quash Subpoena (Rule 17)" (Document No. 31) is **GRANTED**.

Signed: January 16, 2008

**IN THE DISTRICT COURT OF THE UNITED STATES**
**FOR THE WESTERN DISTRICT OF NORTH CAROLINA**
**CHARLOTTE DIVISION**

**CRIMINAL CASE NO. 3:06cr85**

| | | |
|---|---|---|
| **UNITED STATES OF AMERICA,** | ) | |
| | ) | |
| **vs.** | ) | **O R D E R** |
| | ) | |
| **THOMAS McKOY RICHARDSON** | ) | |
| | ) | |

**THIS MATTER** is before the Court on the Defendant's Motion to Suppress [Doc.25] filed July 24, 2007, and Motion by AOL, LLC (AOL) to Quash Subpoena (Rule17) [Doc.31] filed January 4, 2008. Both motions were referred to the Magistrate Judge pursuant to 28 U.S.C. §636. The Magistrate Judge issued a Memorandum and Recommendation [Doc.35] recommending that the Motion to Suppress be denied, to which the Defendant filed timely objections [Doc.39]. The Magistrate Judge entered an Order granting the Motion to Quash [Doc.34], to which the Defendant filed timely objections and

moved the Court to modify or set aside the Order. [Doc.38].

The Defendant having filed timely objections to the Memorandum and Recommendation that the Motion to Suppress be denied, the Court reviews *de novo* the particular recommendation to which objections have been filed. Fed. R. Crim. Pro. Rule 59(b)(3). The Defendant has objected to the Magistrate's recommendation that there was sufficient probable cause for the issuance of the search warrant which led to his arrest. The affidavit in support of that warrant, he argues, was deficient because it contained no allegation that the Defendant had committed any crime at his then current address or that there was a computer located at that address.

Special Agent John White of the North Carolina State Bureau of Investigation (SBI) provided the affidavit in support of the search warrant. [Doc. 25-2, filed July 24, 2007]. He explained in detail the chain of events which led the SBI to suspect that the Defendant was involved with child pornography. In June 2004, the National Center for Missing and Exploited Children (Center) received a complaint from America Online (AOL) that it had discovered the transmission of an e-mail message containing child pornography by a user known as "knifeisland@aol.com" [Id., at ¶10]. The SBI issued an administrative subpoena to AOL and learned that this email address belonged to Thomas M. Richardson living at 2541 Pine View Lane, Apartment H,

Gastonia, N.C. [Id., at ¶11]. When the SBI investigated whether Richardson still lived at that address, it learned that as of August 2004, he did not. [Id., at ¶12]. In September 2005, the Center received another complaint from AOL about an email containing child pornography. [Id., at ¶14]. AOL reported the email address as tr1029@aol.com, an account associated with Thomas Richardson, 8508 Park Road, Charlotte, N.C. [Id., at ¶15-16]. Upon receiving this information, the SBI investigated the current address for Richardson and found that he was living at 7805 Andover Woods Drive, Apartment 604, Charlotte, N.C. [Id., at ¶16]. The investigation also showed, based on Richardson's North Carolina driver's license, that he had used the previous addresses. [Id.]. In addition, the United States Postal Service advised that Richardson now received mail at the Andover Woods address. [Id., at ¶17]. The manager of the apartment complex confirmed that Richardson lived there and his most recent driver's license showed that as his address. [Id., at ¶18-19]. Richardson had a criminal history for sex offenses involving children. [Id., at ¶20-21].

The Defendant argues that this is insufficient to show that at the time of the search warrant, he owned a computer at the Andover Woods apartment or was involved with child pornography at that location. The warrant that issued, he argues, was "a general warrant which could serve as a form or template by merely inserting blanks for the suspect's name, address and a NCMEC report." [Doc. 39, su-

pra., at 2]. And, he argued, the Magistrate completely failed to address the "staleness" issue. [Id.].

Contrary to these statements, the Magistrate Judge cited United States v. Summage, 481 F.3d 1075, 1078 (8 Cir. 2007), a case dealing with almost identical facts. The Eighth Circuit there noted that probable cause sufficient to support a search warrant means a showing of facts, under the totality of the circumstances, to create a "fair probability *that evidence of a crime will be found in the place to be searched.*" Id., at 1077 (emphasis added, citations omitted). There is no requirement that the crime occurred at the place to be searched.

> The date of the occurrence of the facts relied upon in an affidavit is of importance in the determination of probable cause because untimely information may be deemed stale. "There is no bright-line test for determining when information is stale. ... Time factors must be examined in the context of a specific case and the nature of the crime under investigation." Here, ... we conclude that it could be presumed that Summage would maintain in his possession the video and photographs that he made of the sexual encounter between Doe and the waiting woman. Thus, the affidavit's failure to include the date of that encounter is not fatal to a determination that probable cause existed for a search of Summage's new resi-

dence.

Id., at 1078. Likewise, nexus was shown because it was reasonable to infer that Summage would have the video and photographs at his new residence. Id.; *accord*, United States v. Moyer, 2007 WL 4197411 **2 (9th Cir. 2007) ("The chronology of Moyer's subscriptions to two websites devoted to child pornography, his failure to cancel either membership, his prior conviction for distribution of child pornography, and *the common practice of child pornography collectors of storing illegal images on their home computers combine to create a fair probability that downloaded images from the ... websites would be found on Moyer's home computers.*") (emphasis provided).

With regard to the applicability of the good faith exception to the probable cause requirement, the Court finds the Defendant's objections do not warrant *de novo* review. "Having found that the search warrant was valid, the Magistrate Judge naturally found good faith on the part of the law enforcement personnel who presented it." [Doc. 39 at 3]. It is unclear whether this statement is meant to be sarcastic but the assumption that the Magistrate Judge would automatically rule in favor of law enforcement does not warrant discussion.

However, because there was probable cause for the warrant, the issue concerning the good faith exception need not be reached. That portion of

the objection will be overruled as moot, and the portion of the Motion to Suppress concerning the absence of good faith for the search will be denied as moot.

The Defendant also objects to that portion of the Memorandum and Recommendation concerning whether AOL acted as an agent of the government. The Magistrate concluded that AOL routinely scans in order to prevent its network from being used to further child pornography. When such pornography is located, AOL, like all internet providers, is required to report it to the Center. Citing United States v. Jarrett, 338 F.3d 339 (4th Cir. 2003), the Magistrate concluded that the Defendant had failed to meet his burden to show an agency relationship. [Doc. 35 at 9-10].

The Defendant's objection on this point is confusing. He states "Defendant would concede that the facts contained in the Motion to Suppress regarding AOL's relationship and partnership with law enforcement do not, in themselves, establish an agency relationship under the test set forth in [Jarrett]," [Doc. 39, supra], which would appear to negate the objection. Based thereon, however, it appears that Defendant's argument is that AOL's motion to quash the subpoena issued to it by the Defendant was erroneously granted, and without the information which the Defendant would have gleaned from that subpoena, he is unable to meet his burden of proof.

The Court rejects this attempt to bootstrap an objection based on the granting of the motion to quash. The Defendant has conceded the issue and the motion to suppress on the agency issue was properly denied.

The Defendant filed timely objections to the Order of the Magistrate Judge granting the AOL's Motion to Quash and the Court has reviewed the Magistrate Judge's action to determine whether any of the portions objected to are contrary to law or clearly erroneous. Fed. R. Crim. Pro. Rule 59(a). The Court determines that no portion of the Magistrate Judge's Order is contrary to law or clearly erroneous, and that the reasons set forth in that Order are correct and should be affirmed.

**IT IS THEREFORE ORDERED** that the Memorandum and Recommendation of the Magistrate Judge regarding the Motion to Suppress is affirmed and the Objections thereto are overruled and the Motion to Suppress is **DENIED**.

**IT IS FURTHER ORDERED** that the objections to the Order of the Magistrate Judge Quashing the Subpoena to AOL, LLC are **OVERRULED**, and the Defendant's Motion to modify or set aside that Order is **DENIED**.

Signed: March 20, 2008

**42 U.S.C.A. § 13032**
United States Code Annotated
Title 42. The Public Health and Welfare
Chapter 132. Victims of Child Abuse
Subchapter IV. Reporting Requirements

## § 13032. Reporting of child pornography by electronic communication service providers

**(a) Definitions**

In this section--

**(1)** the term "electronic communication service" has the meaning given the term in section 2510 of Title 18; and

**(2)** the term "remote computing service" has the meaning given the term in section 2711 of Title 18.

**(b) Requirements**

(1) Duty to report

Whoever, while engaged in providing an electronic communication service or a remote computing service to the public, through a facility or means of interstate or foreign commerce, obtains knowledge of facts or circumstances from which a violation of section 2251, 2251A, 2252, 2252A, 2252B, or 2260 of Title 18, involving child pornography (as defined in section 2256 of that title), or a violation of section 1466A of that title, is apparent, shall, as soon as reasonably possible, make a report of such facts or circumstances to the Cyber Tip Line at the National Center for Missing and Exploited Children, which

shall forward that report to a law enforcement agency or agencies designated by the Attorney General.

**(2)** Designation of agencies

Not later than 180 days after October 30, 1998, the Attorney General shall designate the law enforcement agency or agencies to which a report shall be forwarded under paragraph (1).

**(3)** In addition to forwarding such reports to those agencies designated in subsection (b)(2), the National Center for Missing and Exploited Children is authorized to forward any such report to an appropriate official of a state or subdivision of a state for the purpose of enforcing state criminal law.

**(4)** Failure to report

A provider of electronic communication services or remote computing services described in paragraph (1) who knowingly and willfully fails to make a report under that paragraph shall be fined--

**(A)** in the case of an initial failure to make a report, not more than $50,000; and

**(B)** in the case of any second or subsequent failure to make a report, not more than $100,000.

**(c) Civil liability**

No provider or user of an electronic communication service or a remote computing service to the public shall be held liable on account of any action taken in good faith to comply with or pursuant to this section.

**(d) Limitation of information or material required in report**

A report under subsection (b)(1) of this section may include additional information or material developed by an electronic communication service or remote computing service, except that the Federal Government may not require the production of such information or material in that report.

**(e) Monitoring not required**

Nothing in this section may be construed to require a provider of electronic communication services or remote computing services to engage in the monitoring of any user, subscriber, or customer of that provider, or the content of any communication of any such person.

**(f) Conditions of disclosure of information contained within report**

**(1)** In general

No law enforcement agency that receives a report under subsection (b)(1) of this section shall disclose any information contained in that report, except that disclosure of such information may be made--

**(A)** to an attorney for the government for use in the performance of the official duties of the attorney;

**(B)** to such officers and employees of the law enforcement agency, as may be necessary in the performance of their investigative and recordkeeping functions;

(C) to such other government personnel (including personnel of a State or subdivision of a State) as are determined to be necessary by an attorney for the government to assist the attorney in the performance of the official duties of the attorney in enforcing Federal criminal law; or

(D) where the report discloses a violation of State criminal law, to an appropriate official of a State or subdivision of a State for the purpose of enforcing such State law.

(2) Definitions

In this subsection, the terms "attorney for the government" and "State" have the meanings given those terms in Rule 54 of the Federal Rules of Criminal Procedure.